UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,703	11/04/2003	Kimitaka Murashita	122.1569	5895

21171 7590 04/04/2007
STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

## *Office Action Summary*	**Application No.** 10/699,703	**Applicant(s)** MURASHITA ET AL.	
	Examiner Jenise E. Jackson	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 February 2006_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-28_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-26_ is/are rejected.

7)☒ Claim(s) _27 and 28_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _20070226_.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-2, 5-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Ortiz et al(2003/0163710).

3. As per claim 1, Ortiz et al discloses a terminal device[i.e. electronic system, 0023] including a biometric data storing unit which stores a plurality of biometric data[such as fingerprint and iris, fig. 9, sheet 9, 0061] associated with a person[0061-0062, 0096], wherein at least one of said biometric data is used to authenticate said person[0114].

4. As per claim 2, Ortiz et al discloses wherein said biometric data includes a plurality of kinds of biometric data[fig. 4 sheet 4, 0027, 0100].

5. As per claim 5, Ortiz et al discloses wherein when performing the authentication of said person, said biometric data to be used to authenticate said person is selected for output from said biometric data storing unit[0024, 0036].

6. As per claim 6, Ortiz et al discloses a biometric data storing unit which stores a plurality

of biometric data associated with a person[0061, 0100, fig. 8 sheet 8]; a biometric data acquisition unit which acquires biometric data[0096]; a person authentication unit which authenticates said person based on said acquired biometric data and said biometric data stored in said biometric data storing unit[0114]; and a biometric data output unit which selects and outputs designated biometric data from said biometric data storing unit when identify of said person has been authenticated by said person authentication unit[0024, 0036].

7. As per claim 7, Ortiz et al discloses a biometric data processing unit which edits and processes at least partially said biometric data selected from said biometric data storing unit, wherein said edited and processed biometric data is output[0123].

8. As per claim 8, Ortiz discloses a biometric data converting unit which converts the format of said biometric data selected from said biometric data storing unit, wherein said format-converted biometric data is output[0032, 0078-0080].

9. As per claim 9, Ortiz discloses a corresponding data generating unit which, from said biometric data selected from said biometric data storing unit, generates corresponding data having a certain bit length and corresponding to said biometric data, wherein said generated corresponding data is output from said biometric data output unit[0087-0089].

10. As per claim 10, Ortiz discloses a corresponding data parameter generating unit which generates a parameter to be used for generating said corresponding data[0073, 0088].

11. As per claim 11, Ortiz et al discloses a terminal device[0023] having a biometric data storing unit which stores a plurality of biometric data associated with a person, and a biometric data transmitting unit which transmits out at least one of said biometric data[0061-0062, 0096, 0100, fig. 9 sheet 9]; and an authentication device having a dictionary data storing unit which

stores biometric data as dictionary data to be matched against[0031, 0114], and a first person authentication unit which performs first person authentication based on said biometric data transmitted from said biometric data transmitting unit and said dictionary data stored in said dictionary data storing unit[0127-0129].

12. As per claim 12, Ortiz et al discloses wherein said biometric data includes a plurality of kinds of biometric data[fig. 4 sheet 4, 0027, 0034, 0100].

13. As per claim 13, Ortiz et al. discloses wherein said terminal device comprises a biometric data acquiring unit which acquires biometric data[0023, 0036, 0086], and a second person authentication unit which performs second person authentication[i.e. iris person authentication, 0105], wherein said second person authentication is performed using said acquired biometric data and said biometric data stored in said biometric data storing unit[see fig. 4 sheet 4] and, when identity of said person has been authenticated[0114], said biometric data to be used in said first person authentication unit[i.e. fingerprint authentication] is transmitted from said biometric data transmitting unit to said authentication device[0105, 0135].

14. As per claim 14, Ortiz discloses wherein said authentication device comprises a corresponding data generating unit which, based on said biometric data transmitted from said biometric data transmitting unit, generates corresponding data having a certain bit length and corresponding to said biometric data, wherein specific dictionary data stored in said dictionary data storing unit is located by using said generated corresponding data, and said first person authentication unit performs said person authentication based on said specific dictionary data and said transmitted biometric data[0087-0089].

15. As per claim 15, Ortiz discloses wherein when said person authentication based on said

specific dictionary data cannot be performed, said authentication device performs said person authentication based on all of said dictionary data stored in said dictionary data storing unit and said transmitted biometric data[0086, 0124].

16. As per claim 16, Ortiz discloses wherein said terminal device includes a first biometric data processing unit which edits and processes at least partially said biometric data selected from said biometric data storing unit[0123], and a first processing data storing unit which stores data that said first biometric data processing unit uses to edit and process said biometric data[0123], and said authentication device includes a second biometric data processing unit which edits and processes said dictionary data at least partially[0105, 0123], and a second processing data storing unit which stores data that said second biometric data processing unit uses to edit and process said dictionary data, and wherein said first person authentication unit performs said person authentication based on said edited and processed biometric data and said edited and processed dictionary data[0105].

17. As per claim 17, Ortiz discloses wherein said authentication device comprises a conversion data storing unit which stores conversion data concerning said biometric data used in said first person authentication unit, and said terminal device comprises a biometric data converting unit which converts the format of said biometric data stored in said biometric data storing unit, and wherein said biometric data converting unit converts the format of said biometric data by using said format data transmitted from said conversion data storing unit, and said format-converted biometric data is transmitted to said authentication device[0078-0080, 0083].

18. As per claim 18, Ortiz discloses a terminal device having a biometric data storing unit

which stores a plurality of biometric data associated with a person[such as fingerprint and iris, fig. 9, sheet 9, 0061], a first corresponding data generating unit which generates corresponding data having a certain bit length and corresponding to specific biometric data selected from along said plurality of biometric data stored in said biometric data storing unit, and a corresponding data transmitting unit which transmits out said generated first corresponding data; and an authentication device having a dictionary data storing unit which holds biometric data[0122, 0124], as dictionary data to be matched against, a second corresponding data generating unit which generates corresponding data having a certain bit length and corresponding to said dictionary data, and a first person authentication unit which performs first person authentication based on said transmitted first corresponding data and said second corresponding data[0087-0089].

19. As per claim 19, Ortiz discloses wherein said terminal device includes a biometric data acquisition unit which acquires biometric data and a second person authentication unit which performs second person authentication[0023, 0105, 0114], and wherein said second person authentication is performed using said acquired biometric data and said biometric data stored in said biometric data storing unit and, when the identity of said person has been authenticated, said first corresponding data to be used in said first person authentication unit is transmitted to said authentication device[0105, 0135].

20. As per claim 20, Ortiz discloses wherein said terminal device includes a first corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and wherein said generated corresponding data parameter is not only used in said first corresponding data generating unit, but also transmitted to

said authentication device and used in said second corresponding data generating unit[0073, 0088].

21. As per claim 21, Ortiz discloses wherein said authentication device includes a second corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and wherein said generated corresponding data parameter is not only used in said second corresponding data generating unit, but also transmitted to said terminal device and used in said first corresponding data generating unit[0073, 0135].

22. As per claim 23, A biometric data acquisition device comprising a biometric data acquiring unit for acquiring a plurality of kinds of biometric data associated with a person[0023, 0036, 0086], and a biometric data storing unit which transfers said biometric data acquired by said biometric data acquiring unit to a terminal device for storage therein[0061-0062, 0096].

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. Claims 3-4, 22, 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ortiz(2003/0163710) in view of Uchida(2001/0025342).

25. As per claim 3, Ortiz et al does not disclose wherein said biometric data is feature point data extracted from biometric data. However, Uchida discloses wherein the biometric data is

feature point data extracted[22, fig 1 sheet 1] from biometric data[0026, 0048]. It would have been obvious to one of ordinary skill in the art at the time of the invention to include the feature point data extracted from biometric data of Uchida with Ortiz, the motivation is that a feature point extractor calculates the feature of biometric data, such as fingerprint data of Uchida and outputs the fingerprinting feature to the fingerprint comparator, for comparison[0048].

26. As per claim 4, Ortiz et al does not disclose wherein said biometric data is encrypted biometric data. However, Uchida discloses wherein the biometric data is encrypted biometric data[0022, 0065]. It would have been obvious of one of ordinary skill in the art at the time of the invention to include biometric data is encrypted biometric data of Uchida with Ortiz, because encrypting biometric data is a protective measure that can enhance security, because even if an unauthorized person steals the biometric data in transit, because the biometric data is encoded[0067 of Uchida] it is intelligible.

27. Same Motivation as claim 4. As per claim 22, Ortiz does not disclose wherein said authentication device encrypts data that said person has by using said corresponding data used for the authentication of said person as an encryption key. Uchida discloses wherein the authentication device encrypts data that the person has by using the corresponding data used for authentication of the person as an encryption key[0022, 0028].

28. Same Motivation as claim 3. As per claim 24, Uchida discloses wherein said biometric data storing unit extracts biometric data feature points from said acquired biometric data and stores said extracted feature points into said terminal device[0026, 0048, 0060].

29. Same Motivation as claim 4. As per claim 25, Uchida discloses wherein said biometric

data storing unit encrypts said acquired biometric data and stores said encrypted biometric data into said terminal device[0022-0023, 0028].

30. As per claim 26, Ortiz discloses a biometric data acquisition system; a terminal device having a biometric data storing unit for storing a plurality of kinds of biometric data [associated with a person such as fingerprint and iris, fig. 9, sheet 9, 0-023, 0061]; an authentication device which performs person authentication based on said biometric data transmitted from said terminal device[0024, 0036, 0114]; and a biometric data acquisition device having a biometric data acquiring unit for acquiring said biometric data[0023, 0036, 0086]. Ortiz does not disclose an encryption unit which encrypts said biometric data by using an encryption key, and a decryption key storing unit which stores a decryption key, and wherein: said biometric data associated with said person, acquired by said biometric data acquiring unit, is encrypted by said encryption unit and transferred to said terminal device for storage in said biometric data storing unit, and when said encrypted biometric data stored in said terminal is transmitted to said authentication device, said authentication device decrypts said encrypted biometric data by using said decryption key stored in said decryption key storing unit of said biometric data acquisition device. Uchida discloses an encryption unit which encrypts said biometric data by using an encryption key[0022], and a decryption key storing unit which stores a decryption key[0030-0031], and wherein: said biometric data associated with said person, acquired by said biometric data acquiring unit, is encrypted by said encryption unit and transferred to said terminal device for storage in said biometric data storing unit[0022, 0028], and when said encrypted biometric data stored in said terminal is transmitted to said authentication device, said authentication device decrypts said encrypted biometric data by using said decryption key stored in said

decryption key storing unit of said biometric data acquisition device[0036]. It would have been obvious to one of ordinary skill in the art to include an encryption key and decryption key in order to perform encryption and decryption of biometric data such as in Uchida with Ortiz, because encrypting biometric data is a protective measure that can enhance security, because even if an unauthorized person steals the biometric data in transit, because the biometric data is encoded[0067 of Uchida] it cannot be read or used without the corresponding decryption key.

Claim Objections

31. Claims 27-28 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims. Claims 27-28 have allowable features, "the decryption key is used by the authentication device, the biometric data acquisition device charges a fee to the authentication device for the use", and "charging a fee to the authentication device according to the number of times that the biometric data stored into the terminal device by the biometric data acquisition device is used by the authentication device". Prior art of record fails to disclose charging a fee for a decryption key, and charging a fee according to the number of times that the biometric data is stored. In prior art, if a user is enrolled in the system, a user is given a decryption key, there is no suggestion or disclosure of a charge to use a decryption key, and no suggestion in prior art as to how many times biometric data is stored.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 29, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100